

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-249921

(43) 公開日 平成11年(1999) 9月17日

(51) Int.Cl.⁶

G 0 6 F 11/10

識別記号

3 3 0

F I

G 0 6 F 11/10

3 3 0 Q

審査請求 未請求 請求項の数 5 O L (全 9 頁)

(21) 出願番号

特願平10-53236

(22) 出願日

平成10年(1998) 3月5日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 花木 義孝

大阪府門真市大字門真1006番地 松下電器

産業株式会社内

(74) 代理人 弁理士 滝本 智之 (外 1 名)

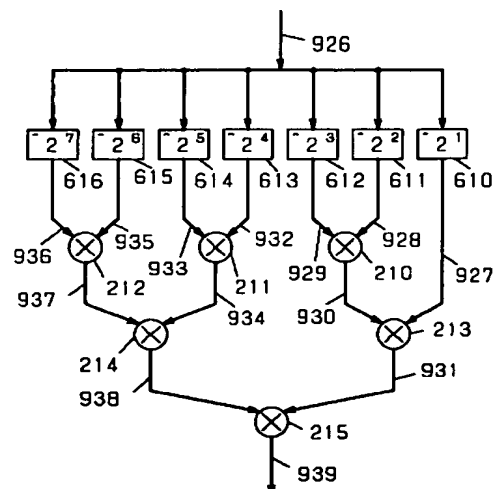
(54) 【発明の名称】 ガロア体演算器

(57) 【要約】

【課題】 ガロア体上の逆元の生成を行うガロア体演算器を実現するにあたり、高速なパイプライン動作を実現しつつ、回路規模の小さなガロア体演算器を実現することを目的とする。

【解決手段】 入力信号をガロア体ベキ乗算回路 610 ~ 616 に入力し、それぞれ 2 乗 ~ 128 乗のベキ乗算をした出力をガロア体乗算器 210 ~ 215 からなるツリーで互いに掛け合わせ、入力の実元を得る。

210~215 ガロア体乗算器
610 ガロア体 2 乗回路
611 ガロア体 4 乗回路
612 ガロア体 8 乗回路
613 ガロア体 16 乗回路
614 ガロア体 32 乗回路
615 ガロア体 64 乗回路
616 ガロア体 128 乗回路



【特許請求の範囲】

【請求項1】 ガロア体 2^n の1乗々回路～ガロア体 2^n の $(n-1)$ 乗々回路と、ツリー状に接続された $n-2$ 個のガロア体乗算器とで構成され、ガロア体 $GF(2^n)$ 上の逆元を生成することを特徴とするガロア体演算器。

【請求項2】 個々のガロア体 2^n の1乗々回路～ガロア体 2^n の $(n-1)$ 乗々回路およびツリー状に接続された $n-2$ 個のガロア体乗算器の、すべてまたはその一部を、それぞれ独立したガロア体 2^n の定数乗々回路およびガロア体乗算器として使用するための選択手段を有することを特徴とする請求項1記載のガロア体演算器。

【請求項3】 ガロア体 2^n の1乗々回路～ガロア体 2^n の $(n-1)$ 乗々回路と、ツリー状に接続された $n-1$ 個のガロア体乗算器とで構成され、ガロア体 $GF(2^n)$ 上の除算を実行することを特徴とするガロア体演算器。

【請求項4】 個々のガロア体 2^n の1乗々回路～ガロア体 2^n の $(n-1)$ 乗々回路およびツリー状に接続された $n-1$ 個のガロア体乗算器の、すべてまたはその一部を、それぞれ独立したガロア体 2^n の定数乗々回路およびガロア体乗算器として使用するための選択手段を有することを特徴とする請求項3記載のガロア体演算器。

【請求項5】 ガロア体 2^n の1乗々回路～ガロア体 2^n の $(n-1)$ 乗々回路と、ツリー状に接続された $n-1$ 個のガロア体乗算器と、個々の前記ガロア体 2^n の1乗々回路～ガロア体 2^n の $n-1$ 乗々回路およびツリー状に接続された $n-1$ 個の前記ガロア体乗算器の、すべてまたはその一部を、それぞれ独立したガロア体 2^n の定数乗々回路およびガロア体乗算器として使用するための選択手段と0個以上のガロア体乗算器と、演算途中のデータを保持するレジスタとで構成され、ガロア体上の多項式の除算をおこなうことを特徴とするガロア体演算器。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 デジタルAVシステムや情報通信などの分野において、誤り訂正符号に関する技術の応用が盛んである。本発明は、誤り訂正符号として有力なリード・ソロモン符号の復号・符号化をおこなうためのガロア体演算器に関するものである。

【0002】

【従来の技術】 従来、ガロア体 $GF(2^n)$ 上の逆元生成器は、逆元ROMと呼ばれるROMによって構成されていた。逆元ROMには、アドレス入力に対してガロア体上の逆元が出力されるようにデータが格納されている。

【0003】 図5に、従来のガロア体上の逆元生成器の構成を示す。同図において、120は逆元ROM、900、901は信号線である。

【0004】 図5の構成によるガロア体逆元生成器の動

作を、以下に説明する。まず、ガロア体演算器への入力が、信号線900を介して、逆元ROM120に入力され、その逆元が逆元ROM120から出力され、信号線901を介してガロア体演算器から出力される。

【0005】 図6に、従来のガロア体除算器の構成を示す。同図において、130は逆元ROM、230はガロア体乗算器、902、903、904、905は信号線である。

【0006】 図6の構成によるガロア体除算器の動作を、以下に説明する。まず、ガロア体除算器へ除数として与えられた入力が、信号線902を介して、逆元ROM130に入力され、その逆元が逆元ROM130から出力され、信号線903を介して、ガロア体乗算器230に入力される。また、ガロア体除算器へ被除数として与えられた入力が、信号線904を介して、ガロア体乗算器230に入力される。ガロア体乗算器230では、除数の逆元と被除数を乗ずることによってガロア体除算の結果が生成され、信号線905を介して、ガロア体除算器から出力される。従来の構成では、以上のようにして、ガロア体除算器を得ていた。

【0007】 図7は、従来のガロア体多項式除算器の構成を示すブロック図である。説明の便宜上、この構成は、ガロア体上の最大3次の除数多項式と最大3次の被除数多項式の除算をおこなうことができるものとしている。図4において、240、241、242はガロア体乗算器、340、341、342はガロア体加算器、440はガロア体除算器、540、541、542、543、544、545、546、547はそれぞれレジスタ、906、907、908、909、910、911、912、913、914、915、916、917、918、919、920、921、922、923、924、925はそれぞれ信号線である。

【0008】 従来のガロア体多項式除算器の動作を、下記の3ステップに分けて説明する。ただし、商多項式 $R(x)$ は、下記のようにあらわされるものとする。

$$【0009】 R(x) = r_{3x^3} + r_{2x^2} + r_{1x} + r_0$$

また、初期状態において、レジスタ540、541、542、543には、それぞれ被除数となる多項式の0

次、1次、2次、3次の係数が格納されており、レジスタ544、545、546、547には、それぞれ除数となる多項式の0次、1次、2次、3次の係数が格納されているものとする。除数多項式は、中間剰余多項式の初期値となる。

【0010】 <ステップ1>まず、除数多項式の最高次の係数が0以外になるように、除数多項式が正規化される。すなわち、レジスタ547の値が0以外になるまで、除数多項式の係数540、541、542、543を低次から高次の方向に1次分ずつシフトする。シフトするときに、最低次の係数を格納するレジスタ544に

3

は、値 0 がシフトインされる。

【0011】<ステップ 2>次に、被除数多項式の最高次係数と、正規化された除数多項式の最高次係数との、ガロア体除算がおこなわれる。ガロア体除算の結果として、商多項式の係数が 1 次分だけ求まる。すなわち、レジスタ 5 4 3 の値が信号線 9 1 2 を介してガロア体除算器 4 4 0 に入力されており、正規化された除数多項式の最高次の係数を格納するレジスタ 5 4 7 の値が信号線 9 1 6 を介してガロア体除算器 4 4 0 に入力されている。ガロア体除算器 4 4 0 では、被除数の最高次係数を被除数とし、除数の最高次係数を除数とする除算がおこなわれる。除算結果は、商多項式 $R(x)$ の最高次係数 $r_{deg(R(x))}$ として、信号 9 2 5 を介して出力される。

【0012】<ステップ 3>次に、<ステップ 1>で正規化された除数多項式の各係数と、<ステップ 2>で求めた商多項式の 1 次分の係数とのガロア体乗算をおこない、その結果と、これまでに求めた中間剰余多項式とのガロア体加算をおこなうという、ガロア体積和演算がおこなわれる。ガロア体積和演算の結果は、次の中間剰余多項式となる。すなわち、信号 9 2 5 が、ガロア体乗算器 2 4 0、2 4 1、2 4 2 に入力されている。また、レジスタ 5 4 4、5 4 5、5 4 6 から、それぞれ除数多項式の 0 次、1 次、2 次の係数が、それぞれ信号線 9 1 3、9 1 4、9 1 5 を介して、それぞれガロア体乗算器 2 4 0、2 4 1、2 4 2 へ入力されており、ガロア体除算器 4 4 0 の出力と乗ぜられ、それぞれ信号 9 2 0、9 2 1、9 2 2 を介してガロア体加算器 3 4 0、3 4 1、3 4 2 に入力される。また、レジスタ 5 4 0、5 4 1、5 4 2 の値がそれぞれ信号線 9 0 6、9 0 8、9 1 0 を介してガロア体加算器 3 4 0、3 4 1、3 4 2 に入力され、それぞれ信号線 9 2 0、9 2 1、9 2 2 の値と加算され、それぞれ信号線 9 0 7、9 0 9、9 1 1 を介してレジスタ 5 4 1、5 4 2、5 4 3 に格納される。レジスタ 5 4 0 には、値 0 が格納される。

【0013】<ステップ 2>と<ステップ 3>を繰り返すことによって、<ステップ 2>が実行されるたびに、商多項式の係数が 1 次分ずつ、 $r_{deg(R(x))}$ 、 $r_{deg(R(x))-1}$ 、 $r_{deg(R(x))-2}$ 、 \dots 、 r_1 、 r_0 、という順に、信号 9 2 5 から出力される。必要があれば、この出力をシリアル-パラレル変換することによって、商多項式を求めることができる。剰余多項式は、<ステップ 2>で r_0 が求めた直後の<ステップ 3>を実行したときに、レジスタ 5 4 0、5 4 1、5 4 2、5 4 3 に格納されている中間剰余多項式として得られる。レジスタ 5 4 0、5 4 1、5 4 2、5 4 3 にそれぞれ、0 次、1 次、2 次、3 次の係数が得られる。

【0014】このようにして、従来のガロア体多項式除算器では、<ステップ 1>除数多項式の正規化と、<ス

4

テップ 2>ガロア体除算および<ステップ 3>ガロア体積和演算の繰り返しによって、ガロア体多項式除算の結果を得ていた。

【0015】

【発明が解決しようとする課題】以下に、上記ガロア体演算器の構成における課題について説明する。従来の構成では、ガロア体上の逆元を生成するため、あるいは、ガロア体上の除算を実行するためには、ガロア体上の逆元を記憶した ROM が必要であった。そのため、ガロア体演算器にパイプライン構造をもたせて、ROM のアクセス速度以上のスループットを実現するには、複数の ROM をインターリーブさせる必要があり、高速なパイプライン動作を実現しつつ回路規模の小さなガロア体演算器を得るのが困難である、という課題があった。また、ガロア体の原始多項式に対応した逆元 ROM が必要であるため、複数の原始多項式に対応するためには、原始多項式の数と同数の逆元 ROM が必要となる。そのため、複数の原始多項式に対応しつつ回路規模の小さなガロア体演算器を得るのが困難である、という課題があった。また、ガロア体上の逆元を記憶するための専用 ROM を実装する必要があるため、ゲートアレイや FPGA など

に実装するのが困難である、という課題があった。【0016】また、従来の構成では、ガロア体除算とガロア体乗算の双方を必要とするガロア体演算器を構成する場合に、ガロア体除算器とガロア体乗算器の双方を実装する必要があり、回路規模が小さなガロア体演算器を構成するのが困難である、という課題があった。

【0017】また、従来の構成では、最高次数 m のガロア体上の多項式の除算を実現するには、ガロア体除算器と、 $m-1$ 個のガロア体乗算器が必要であった。回路規模が大きなガロア体除算器に加えて、 $m-1$ 個もの多数のガロア体乗算器を持つ必要があるため、回路規模の小さなガロア体上の多項式の除算器を得るのが困難である、という課題があった。また、ガロア体除算器として、ガロア体上の逆元を記憶するための ROM を持つ前記従来のガロア体除算器を使用するため、従来のガロア体上の除算器についてこれまでに述べた課題のすべてが、従来のガロア体上の多項式の除算器にも当てはまった。

【0018】本発明は、上記のような従来の課題を解決するものであり、ガロア体上の逆元の生成、あるいは、ガロア体上の除算をおこなうガロア体演算器を実現するにあたり、高速なパイプライン動作を実現しつつ回路規模の小さなガロア体演算器を提供すること、および、複数の原始多項式に対応しつつ回路規模の小さなガロア体演算器を提供すること、および、ゲートアレイや FPGA などにも容易に実装可能なガロア体演算器を提供することを目的とする。

【0019】また、本発明は、ガロア体除算器とガロア体乗算器の双方を含みつつ、回路規模の小さなガロア体

演算器を提供することを目的とする。

【0020】また、本発明は、ガロア体上の多項式の除算を実現するための、小規模なガロア体演算器を提供することを目的とする。

【0021】

【課題を解決するための手段】本発明の請求項1記載の、ガロア体上の逆元を生成するガロア体演算器は、ガロア体 $GF(2^n)$ 上において、前記ガロア体演算器の入力をそれぞれ入力とするようなガロア体2の1乗々回路～ガロア体2の $(n-1)$ 乗々回路と、前記ガロア体2の1乗々回路～ガロア体2の $(n-1)$ 乗々回路の出力すべてを掛けあわせるようにツリー状に接続された $n-2$ 個のガロア体乗算器とで構成されることを特徴とする。

【0022】この構成では、ガロア体 $GF(2^n)$ 上のガロア体演算は、 $(n-1)$ 個の項の総乗となっている。 $(n-1)$ つの項の総乗は、たかだか $(\log(n-1)) + 1$ 段の乗算器のツリーで構成することが可能である（ただし、対数の底は2。以下同じ）。よって、この構成から、ガロア体上の逆元生成回路を、 $(\log(n-1)) + 1$ 段のパイプラインステージに、容易に分割することができる。

【0023】さらに、ガロア体乗算器は、回路規模をさほど増大させることなく、対応する原始多項式の数が増大させることが可能である。よって、この構成によれば、複数の原始多項式に対応しつつ、小規模なガロア体演算器を得ることができる。

【0024】さらに、この構成では、ガロア体演算器全体をランダムロジックで構成することが可能である。よって、ゲートアレイやFPGAなどにも容易に実装することが可能である。

【0025】本発明の請求項2記載のガロア体演算器は、請求項1記載のガロア体演算器を構成する、個々のガロア体2の定数乗々回路および $(n-2)$ 個のガロア体乗算器の、すべてまたはその一部を、それぞれ独立したガロア体2の定数乗々回路およびガロア体乗算器として使用するための選択手段を有することを特徴とする。

【0026】この構成によれば、ガロア体の逆元生成器とガロア体乗算器とガロア体2の定数乗々回路をもつような場合と比較して、回路規模の小さなガロア体演算器を得ることができる。

【0027】本発明の請求項3記載の、ガロア体上の除算をおこなうガロア体演算器は、ガロア体 $GF(2^n)$ 上において、ガロア体演算器の除数を入力とするガロア体2の1乗々回路～ガロア体2の $(n-1)$ 乗々回路と、前記ガロア体2の1乗々回路～ガロア体2の $(n-1)$ 乗々回路とガロア体演算器の被除数のすべてを掛け合わせるようにツリー状に接続された $n-1$ 個のガロア体乗算器とで構成されることを特徴とする。

【0028】なお、これはガロア体 $GF(2^n)$ 上の

元 a 、 b について、以下の等式が成立するという代数的な性質に基づいている：

$$b \div a = b \times a^{-1} = b \times a^{-(2^{n-1})} \times a^{-(2^{n-2})} \times \cdots \times a^{-(2^1)} \times a^{-(2^0)}$$

この構成では、前記本発明の請求項1で述べたような、複数段のステージを持つパイプラインに容易に分割することが可能であり、複数の原始多項式に対応しつつ、小規模なガロア体演算器を得ることが可能であり、かつ、ゲートアレイやFPGAなどにも容易に実装することが可能である、という議論がそのまま当てはまる。

【0029】本発明の請求項4記載のガロア体演算器は、請求項3記載のガロア体演算器を構成する、個々のガロア体2の定数乗々回路および個のガロア体乗算器の、すべてまたはその一部を、それぞれ独立したガロア体2の定数乗々回路およびガロア体乗算器として使用するための選択手段を有することを特徴とする。

【0030】この構成によれば、ガロア体の逆元を生成したり、ガロア体の除算を実行する必要がないサイクルに、ガロア体2の定数乗々回路、および、ガロア体乗算器として、ガロア体演算器を利用することができる。従って、回路規模の小さなガロア体演算器を得ることができる。

【0031】本発明の請求項5記載のガロア体演算器は、本発明の請求項4のガロア体演算器と、0個以上のガロア体乗算器と、演算途中のデータを保持するレジスタとで構成され、ガロア体上の多項式の除算をおこなうことを特徴とする。

【0032】すでに従来の技術の欄で述べたように、最高 m 次のガロア体上の多項式の除算をおこなうには、ガロア体の除算と、相互に並列に実行可能な $m-1$ 回のガロア体乗算とを、交互に繰り返す必要がある。本発明の請求項5の構成によれば、本発明の請求項4で述べたガロア体 $GF(2^n)$ 上のガロア体演算器をガロア体除算器として使用するサイクルと、独立した $n-1$ 個のガロア体乗算器として使用するサイクルとを、交互に繰り返すことによって、ガロア体除算をおこなうことが可能である。このとき、ガロア体除算器と、 $m-1$ 個のガロア体乗算器とを共用することが可能となり、回路規模の小さなガロア体上の多項式の除算器を得ることが可能となる。

【0033】

【発明の実施の形態】以下、本発明の実施の形態について、図面を参照しながら説明する。

【0034】（実施の形態1）まず、本発明の実施の形態1のガロア体演算器について説明する。

【0035】図1は、本実施の形態1のガロア体演算器の構成を示すブロック図である。図1のガロア体演算器は、ガロア体上の逆元を生成する。説明の便宜上、図1にはガロア体 $GF(2^8)$ 上のガロア体演算器を示している。

【0036】図1において210、211、212、213、214、215はガロア体乗算器、610はガロア体2乗回路、611はガロア体4乗回路、612はガロア体8乗回路、613はガロア体16乗回路、614はガロア体32乗回路、615はガロア体64乗回路、616はガロア体128乗回路、926、927、928、929、930、931、932、933、934、935、936、937、938、939はそれぞれ信号線である。

【0037】以上のように構成された実施の形態1のガロア体演算器の動作を、以下に説明する。まず、ガロア体演算器の入力が信号線926を介してガロア体2乗回路610、ガロア体4乗回路611、ガロア体8乗回路612、ガロア体16乗回路613、ガロア体32乗回路614、ガロア体64乗回路615、ガロア体128乗回路616に入力され、それぞれ2乗、4乗、8乗、16乗、32乗、64乗、128乗されて、それぞれ信号線927、928、929、932、933、935、936を介して、ガロア体乗算器210、211、212、213、214、215からなるガロア体乗算器のツリーで互いに掛け合わせられ、信号線939から乗算結果が出力される。この乗算結果は、ガロア体演算器の入力を2乗、4乗、8乗、16乗、32乗、64乗、128乗したものを、それぞれ掛け合わせた数となる。これはガロア体演算器の入力の逆元である。

【0038】（実施の形態2）次に、本発明の実施の形態2のガロア体演算器について説明する。

【0039】図2は、本実施の形態2のガロア体演算器の構成を示すブロック図である。同図のガロア体演算器は、ガロア体上の除算をおこなう。説明の便宜上、図5にはガロア体GF(2⁸)上のガロア体演算器を示している。

【0040】図5において250、251、252、253、254、255、256はそれぞれガロア体乗算器、650はガロア体2乗回路、651はガロア体4乗回路、652はガロア体8乗回路、653はガロア体16乗回路、654はガロア体32乗回路、655はガロア体64乗回路、656はガロア体128乗回路、940、941、942、943、944、945、946、947、948、949、950、951、952、953、954、955はそれぞれ信号線である。

【0041】以上のように構成された実施の形態2のガロア体演算器の動作を、以下に説明する。まず、ガロア体演算器の被除数が信号線941を介してガロア体乗算器250に入力される。また、ガロア体演算器の除数が信号線940を介してガロア体2乗回路650、ガロア体4乗回路651、ガロア体8乗回路652、ガロア体16乗回路653、ガロア体32乗回路654、ガロア体64乗回路655、ガロア体128乗回路656に入力され、それぞれ2乗、4乗、8乗、16乗、32乗、64

乗、128乗されて、それぞれ信号線942、944、945、948、949、951、952を介して、ガロア体乗算器250、251、252、253、254、255、256からなるガロア体乗算器のツリーに入力され、ガロア体演算器の被除数とともに掛け合わせられ、信号線955から乗算結果が出力される。この乗算結果は、ガロア体演算器の被除数、および、除数を2乗、4乗、8乗、16乗、32乗、64乗、128乗したものをそれぞれ掛け合わせた数、すなわちガロア体演算器の被除数を除数で割った除算結果である。

【0042】（実施の形態3）次に、本発明の実施の形態3のガロア体演算器について説明する。

【0043】図3は、本実施の実施の形態3のガロア体演算器の構成を示すブロック図である。同図のガロア体演算器は、選択信号の値に応じて、ガロア体GF(2^m)上のガロア体除算器として動作するか、あるいは、各々独立したガロア体2の1乗乗回路～ガロア体2の(m-1)乗乗回路と複数のガロア体乗算器として動作するかを切り替えることが可能である。説明の便宜上、図3はガロア体GF(2⁴)上のガロア体演算器の場合について示している。すなわち、同図において、m=4である。

【0044】図3において、260、261、262はガロア体乗算器、660はガロア体2乗回路、661はガロア体4乗回路、662はガロア体8乗回路、760、761、762、763、764、765、766はセクタ、956、957、958、959、960、961、962、963、964、965、966、967、968、969、970、971、972、973、974、975、976、977、978はそれぞれ信号線である。979は選択信号の加わる信号線である。

【0045】以上のように構成された実施の形態3のガロア体演算器の動作を以下に説明する。まず、信号線979に加わる選択信号が1である場合について説明する。このとき、図6のガロア体演算器は、ガロア体除算器として動作する。まず、ガロア体除算の被除数が信号線956を介して、セクタ760、761、762に入力され、選択信号が1であるので選択・出力され、信号線957、960、963を介して、ガロア体2乗回路660、ガロア体4乗回路661、ガロア体8乗回路662に入力される。ガロア体除算の被除数を2乗、4乗、8乗した値が、それぞれガロア体2乗回路660、ガロア体4乗回路661、ガロア体8乗回路662から出力され、それぞれ信号線958、961、964を介してセクタ767、764、765に入力され、選択信号が1であるので選択・出力され、それぞれ信号線980、962、965を介して、ガロア体乗算器261、260、260へ入力される。また、ガロア体除算の除数が信号線976を介してガロア体乗算器961に

入力される。選択信号が 1 であるとき、ガロア体乗算器 2 6 0、2 6 1、2 6 2 はガロア体乗算のツリーを構成している。これまでの動作でガロア体除算の被除数の 2 乗、4 乗、8 乗、およびガロア体除算の除数がガロア体乗算のツリーに入力されており、これらを掛け合わせた値、すなわちガロア体除算の結果が信号線 2 6 2 を介して出力される。

【0 0 4 6】次に、信号線 9 7 9 に加わる選択信号が 0 である場合、図 3 に示したガロア体演算器は、各々 1 個のガロア体 2 乗回路、ガロア体 4 乗回路、ガロア体 8 乗回路、および 3 個のガロア体乗算器として動作する。

【0 0 4 7】（実施の形態 4）次に、本発明の実施の形態 4 のガロア体演算器について説明する。

【0 0 4 8】図 4 は、本発明の実施の形態 4 のガロア体演算器の構成を示すブロック図である。同図のガロア体演算器は、図 7 で示したガロア体多項式除算器の構成において、ガロア体除算器 4 4 0 および 3 個のガロア体乗算器 2 4 0、2 4 1、2 4 2 を、発明の実施の形態 3 で述べた図 3 で示したガロア体演算器で置き換え、かつガロア体除算の結果を格納するためのレジスタを追加した構成をしている。本発明の実施の形態 4 のガロア体多項式除算器の動作を、下記の 3 ステップに分けて説明する。ただし、商多項式 $R(x)$ は、下記のようにあらわされるものとする。

$$【0 0 4 9】R(x) = r_3 x^3 + r_2 x^2 + r_1 x + r_0$$

また、初期状態において、レジスタ 5 7 0、5 7 1、5 7 2、5 7 3 には、それぞれ被除数となる多項式の 0 次、1 次、2 次、3 次の係数が格納されており、レジスタ 5 7 4、5 7 5、5 7 6、5 7 7 には、それぞれ除数となる多項式の 0 次、1 次、2 次、3 次の係数が格納されているものとする。除数多項式は、中間剰余多項式の初期値となる。

【0 0 5 0】<ステップ 1> まず、除数多項式の最高次の係数が 0 以外になるように、除数多項式が正規化される。すなわち、レジスタ 5 7 7 の値が 0 以外になるまで、除数多項式の係数 5 7 0、5 7 1、5 7 2、5 6 3 を低次から高次の方向に 1 次分ずつシフトする。シフトするときに、最低次の係数を格納するレジスタ 5 7 4 には、値 0 がシフトインされる。

【0 0 5 1】<ステップ 2> 次に、本発明の実施例を構成する本発明の実施の形態 3 で述べたガロア体演算器がガロア体除算器として動作するような値が選択信号に印加され、被除数多項式の最高次係数と、正規化された除数多項式の最高次係数との、ガロア体除算がおこなわれる。ガロア体除算の結果として、商多項式の係数が 1 次分だけ求まる。また、ガロア体除算の結果は、レジスタに記憶され、<ステップ 3> での利用に備えられる。すなわち、選択信号 1 0 0 5 には、値 1 が印可され、セレクト 7 7 0、7 7 1、7 7 2、7 7 3、7 7 4、7 7

5、7 7 6 に入力される。これによって、本発明の実施の形態 3 で述べたガロア体演算器 4 7 0 は、ガロア体除算器として動作する。また、レジスタ 5 7 3 の値が信号 1 0 0 3 を介してガロア体演算器 4 7 0 に入力されており、正規化された除数多項式の最高次の係数を格納するレジスタ 5 7 7 の値が信号 9 9 1 とセレクト 7 7 0 を介してガロア体演算器 4 7 0 へ入力されている。ガロア体演算器 4 7 0 では、被除数の最高次係数を被除数とし、除数の最高次係数を除数とする除算がおこなわれる。除算結果は、商多項式 $R(x)$ の最高次係数 $r_deg(R(x))$ として、信号線 1 0 0 1 を介して出力される。また、 $r_deg(R(x))$ の値は、レジスタ 5 7 8 に格納され、<ステップ 3> での利用に備えられる。

【0 0 5 2】<ステップ 3> 次に、本発明の実施例を構成する、本発明の実施の形態 3 で述べたガロア体演算器が 3 個のガロア体乗算器として動作するような値が選択信号に印加され、<ステップ 1> で正規化された除数多項式の各係数と、<ステップ 2> で求めた商多項式の 1 次分の係数とのガロア体乗算をおこない、その結果と、これまで求めた中間剰余多項式とのガロア体加算をおこなうという、ガロア体積和演算がおこなわれる。ガロア体積和演算の結果は、次の中間剰余多項式となる。すなわち、信号線 1 0 0 5 に加わる選択信号に値 0 が印加される。これによって、本発明の実施の形態 3 で述べたガロア体演算器 4 7 0 は、3 個のガロア体乗算器として動作する。次に、<ステップ 2> で求めたレジスタ 5 7 8 の値が信号線 1 0 0 2 と、セレクト 7 7 5、7 7 4、7 7 2 を介して、それぞれガロア体乗算器 2 7 0、2 7 1、2 7 2 に入力されている。また、レジスタ 5 7 4、5 7 5、5 7 6 から、それぞれ除数多項式の 0 次、1 次、2 次の係数が、それぞれ信号線 9 8 8、9 8 9、9 9 0 を介して、それぞれガロア体乗算器 2 7 0、2 7 1、2 7 2 へ入力されており、レジスタ 5 7 8 の出力と乗ぜられ、それぞれ信号線 1 0 0 1、1 0 0 6、1 0 0 7 を介してガロア体加算器 3 7 0、3 7 1、3 7 2 に入力される。また、レジスタ 5 7 0、5 7 1、5 7 2 の値がそれぞれ信号線 9 8 2、9 8 4、9 8 6 を介してガロア体加算器 3 7 0、3 7 1、3 7 2 に入力され、それぞれ信号線 1 0 0 1、1 0 0 6、1 0 0 7 の値と加算され、それぞれ信号線 9 8 3、9 8 5、9 8 7 を介してレジスタ 5 7 1、5 7 2、5 7 3 に格納される。レジスタ 5 7 0 には、値 0 が格納される。

【0 0 5 3】<ステップ 2> と <ステップ 3> を繰り返すことによって、<ステップ 2> が実行されるたびに、商多項式の係数が 1 次分ずつ、 $r_deg(R(x))$ 、 $r_deg(R(x)) - 1$ 、 $r_deg(r(x)) - 2$ 、…、 r_1 、 r_0 、という順に、信号 1 0 0 1 から出力される。必要があれば、この出力をシリアル-パラレル変換することによって、商

多項式を求めることができる。剰余多項式は、＜ステップ 2＞で r_0 が求まった直後の＜ステップ 3＞を実行したときに、レジスタ 570、571、572、573 に格納されている中間剰余多項式として得られる。レジスタ 570、571、572、573 にそれぞれ、0 次、1 次、2 次、3 次の係数が得られる。

【0054】このようにして、本発明の実施の形態 4 のガロア体多項式除算器では、＜ステップ 1＞除数多項式の正規化と、＜ステップ 2＞ガロア体除算および＜ステップ 3＞ガロア体積和演算の繰り返しによって、ガロア体多項式除算の結果を得る。

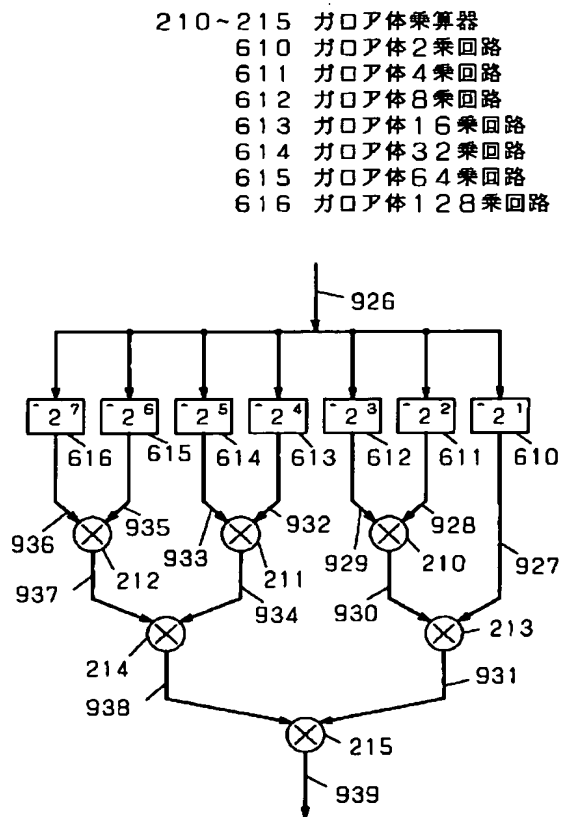
【0055】

【発明の効果】以上のように本発明によれば、ガロア体ベキ乗々回路と、ツリー状に接続されたガロア体乗算器とを備えることにより、回路規模を増大させることなくパイプライン化が可能で、回路規模を増大させることなく複数の原始多項式に対応し、ゲートアレイや F P G A などにも容易に実装することが可能なガロア体逆元生成器を得ることができる。

【図面の簡単な説明】

【図 1】本発明の実施の形態 1 に係るガロア体逆元生成

【図 1】



器の構成を示すブロック図

【図 2】本発明の実施の形態 2 に係るガロア体除算器の構成を示すブロック図

【図 3】本発明の実施の形態 3 に係るガロア体演算器の構成を示すブロック図

【図 4】本発明の実施の形態 4 に係るガロア体多項式除算器の構成を示すブロック図

【図 5】従来のガロア体逆元生成器の構成を示すブロック図

10 【図 6】従来のガロア体除算器の構成を示すブロック図

【図 7】従来のガロア体多項式除算器の構成を示すブロック図

【符号の説明】

210~215 ガロア体乗算器

610 ガロア体 2 乗回路

611 ガロア体 4 乗回路

612 ガロア体 8 乗回路

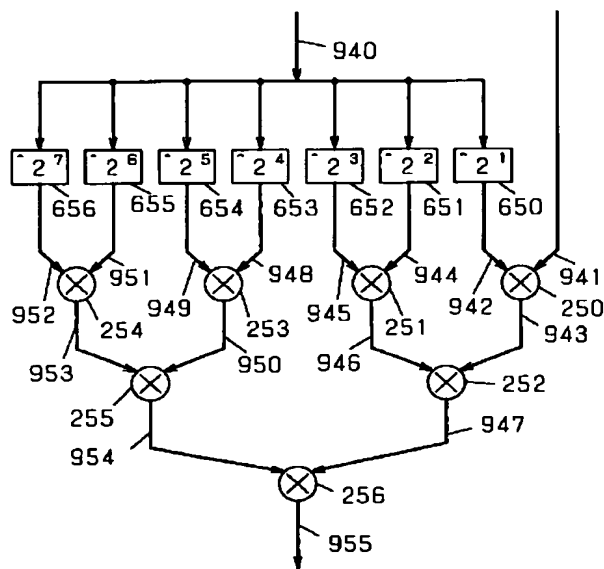
613 ガロア体 16 乗回路

614 ガロア体 32 乗回路

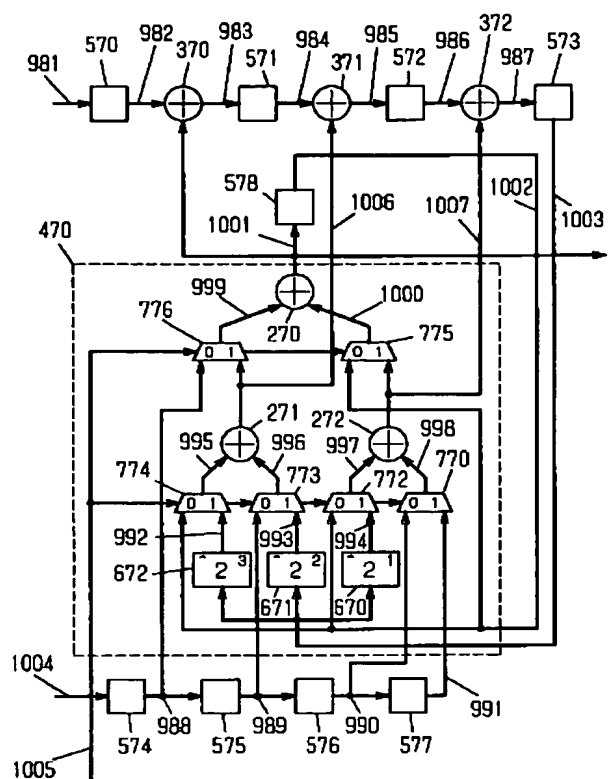
20 615 ガロア体 64 乗回路

616 ガロア体 128 乗回路

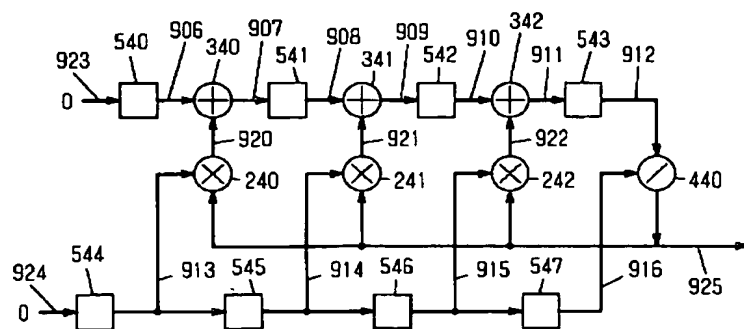
【図 2】



【図4】



【図 7】



【図 6】

